те: официальный сайт. 2014. URL: http://portal.tpu.ru/departments/otdel/stbi/Tab1 (дата обращения: 14.10 2014 г.).

3. Программа поддержки и развития молодежного предпринимательства «Молодежный бизнес России» в Новосибирской области [Электронный ресурс] // Новосибирская торгово-промышленная палата. 2014. URL: http://www.ntpp.ru/dopolnitelno/podderzhka_molodezhnogo_predprinimatelstva/index.html (дата обращения: 13.10 2014 г.).

4. Россия сегодня (факты и цифры за последние 20 лет) // Справочно-информационные материалы для преподавателей вузов. – М., 2012. – 9 с.

ПРОБЛЕМЫ СОХРАННОСТИ ЛИЧНЫХ ДАННЫХ СОТРУДНИКОВ В ОРГАНИЗАЦИИ

Я.В. Савельева

Томский Политехнический Университет, г. Томск
E-mail: yanochka29@mail.ru
Научный руководитель: Роготнева Е.Н., канд, фил. наук, доцент

Каждый человек обладает личной информацией, который в праве, распоряжаться только он сам. К персональным данным человека относится не только рост и вес, но и данные о его рождении, место проживания, образование, серия и номер паспорта, которые в современном обществе от нас требуют в каждой организации. А на сколько, защищены наши персональные данные, при передаче их иному лицу? Кто несет ответственность за безопасное хранение данной информации?

Персональными данными принято считать любую информацию, не смотря на то, косвенно или прямо она относится к определенному или определяемому физическому лицу, то есть к субъекту персональных данных.

Защита персональных данных осуществляется на нормативной основе, а именно: Конституция РФ, Федеральный закон «О персональных данных», Указ Президента РФ «О перечне сведений конфиденциального характера» и другие акты. Правовой основой послужила Всеобщая декларация прав человека, которая была провозглашена Генеральной Ассамблеей Организации Объеденных Наций в 1948 году. Согласно ст. 12 этого документа «никто не имеет права подвергаться произвольному вмешательству в его личную и семейную жизнь произвольным посягательством на его честь и репутацию». [4]

Одной из базовых проблем защиты персональных данных является Федеральный закон Российской Федерации от 27 июля 2006 г. 152-ФЗ «О персональных данных». Закон был принят в целях исполнения международных обязательств Российской Федерации, которые возникли после подписания Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г.

Данная конвенция, а также Федеральный закон «О персональных данных» обладают основными требованиями, одним из которых является взятие с физического лица его согласия на обработку персональных данных. [7]

Уровень защиты, а также новые типы информационных систем определяется Постановлением Правительства РФ от 1 ноября 2012 г., №1119 Москва "Об утвер-

ждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Документ должен быть подписан Федеральной службой безопасности РФ и Федеральной службой по техническому и экспортному контролю (ФСТЭК). В пределах компетенции органов исполнительной власти утверждаются нормативные правовые акты, а также методические документы, которые необходимы для выполнения требований, предусмотренных Положением.

Приказ ФСТЭК России от 18 февраля 2013 г. №21, Москва «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Данный документ был зарегистрирован 14 мая 2013 г., а опубликован 22 мая 2013 г. в «Российской газете» (№ 6083). Закон вступил в силу с 1 июня 2013 года.

Таким образом, приказ ФСТЭК России от 5 февраля 2010 г. №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» утратил юридическую силу.

Рассматривая Федеральный закон №363-ФЗ, который представляет собой внесенные изменения в Федеральный закон «О персональных данных», вступивший в действие с 29 декабря 2009г., исключается требование при обработке шифровальных средств оператором. Разработанные требования методических материалов ФСБ РФ, которые направлены на разъяснение требований по обеспечению безопасности обязательного характера не имеют.

Рассматривая законы Российской Федерации, можно отметить, что зачастую происходит изменение требований к государственным и частным компаниям, а так же организациям и физическим лицам, обладающими (сбор, хранение, обработка и передача данных) персональными данными. Данные организации, компании и физические лица относятся к операторам персональных данных.

Изучив закон «О персональных данных», можно выделить несколько действий, не распространяющихся на отношения. Такие действия могут возникнуть в результате обработки персональных данных в личных или семейных целях, при условии того, что не будут затронуты и нарушены права субъекта. Документы Архивного Фонда Российской Федерации, а также другие архивные документы, которые подлежат организации комплектования, учета, использования и хранения в соответствии с законодательными актами об архивном деле Российской Федерации. Не распространяются на отношения и сведения, относящиеся к государственной тайне, а также обработка персональных данных. Документы, подлежащие обработке включены в единый реестр о физических лицах и индивидуальных предпринимателей. Обработка такого типа осуществляется в соответствии с законом. [7]

Руководствуясь законом, подзаконными актами, а также документами регулирующих органов (ФСБ РФ, ФСТЭК), операторы персональных данных выполняют ряд требований по защите информации своих сотрудников либо клиентов (физических лиц), которые проходят обработку через базу данных организации. Таким образом, операторы предпринимают следующие действия: во-первых, в соответствии с Законом №152-ФЗ ст.22, направляется уведомление об обработке личных данных физического лица. Во-вторых, необходимо получить письменное согласие субъекта на разрешение обработки своих персональных данных, что прописано в Федеральном законе «О персональных данных» ст.9. В результате проделанной работы, исхо-

дя из закона №152-ФЗ ст.21, субъект должен быть, уведомлен о прекращении и уничтожении обработки персональных данных.

В исключительном случае, при условии трудовых отношений между оператором персональных данных и субъектом, либо иных договорных отношениях, которые указаны в Федеральном законе «О персональных данных» №152-ФЗ (ст.6 п.2 и ст.22 п.2), письменное согласие и уведомление субъекта не требуется. [7]

На основании Конституции РФ, Трудового кодекса РФ, Уголовного кодекса РФ, Гражданского кодекса РФ, а так же исходя из Федерального закона «Об информации, информатизации и защите информации», было создано Положение, цель которого, состоит в защите персональных данных сотрудника организации от неправомерного и несанкционированного доступа, а также использования или утраты информации. Данное Положение действует с момента подписания Приказа генеральным директором организации, а также является обязательным в исполнении, для всех сотрудников, которые имеют доступ к персональным данным работников.

Персональные данные физического лица носят конфиденциальный характер, срок хранения данных такого типа составляет 75 лет, либо истекает в случае обезличивания, если иные условия не прописаны в законодательных актах. [5]

Для любого работодателя персональные данные сотрудника организации являются необходимой информацией, в результате заключения с ним трудового договора, что непосредственно касается любого работника. В данном случае, под персональными данными сотрудника принято считать сведения о его жизни, фактах и иных событиях, которые позволяют анализировать личность работника.

К личным данным сотрудника организации относятся: данные об образовании, а также трудовом и общем стаже, содержание трудового договора, личные дела и трудовые книжки работника, сведения о составе семьи и заработной плате сотрудника, наличие материальных ценностей, подача деклараций в налоговую инспекцию. Особо важными стоит отметить: паспортные данные, воинская обязанность, сведения о специальности и занимаемой должности, а так о возможных социальных льготах. Дела, которые содержат информацию о дополнительных курсах, переподготовке, аттестации или повышения квалификации сотрудника. Во многих муниципальных учреждениях или крупных организациях очень важное место занимают сведения о наличии судимостей работника или членов его семьи. Работодателю известно место работы или учебы членов семьи, домашний адрес и телефон, а также характер взаимоотношений семьи работника. [5]

Данного рода документы носят конфиденциальный характер, но исходя из условий единого места обработки и хранения документов, а также их массовости – гриф ограничения не ставится.

Все личные данные сотрудников проходят стадию обработки, к которой относится получение информации, сортировка, комбинирование и хранение, а также передача или использование сведений о работнике.

В целях обеспечения безопасности, учитывая при обработке данных права и свободы человека и гражданина, работодатель должен соблюдать определенные требования:

- Обработка личной информации сотрудника должна осуществляться в целях личной безопасности работника, соблюдение нормативно-правовых актов, его обучении, переподготовке или повышения квалификации, а также контроля и качества выполняемой работы, а также сохранности имущества.

- Получение личных данных о сотруднике может осуществляться двумя способами, а именно: путем представления данных от лица работника, либо поиском информации иным путем с помощью различных источников и баз данных.
- Прежде всего, личные данные работника необходимо получать от его лица. Если получение и проверка информации происходит иным путем, сотрудника заранее должны поставить в известность, получив от его лица письменное согласие. Субъекту персональных данных обязаны сообщить цель получения личной информации, а также предполагаемые источники и способы поиска данных.
- Не должна быть затронута частная жизнь сотрудника, а именно, его политические и религиозные убеждения, мировоззрение и прочее. Также не обрабатывается информация о профсоюзной деятельности и общественных объединениях, если это не предусмотрено законом. Информация такого рода может быть предоставлена работником в случае трудовых отношений от своего лица, либо с письменного согласия.

Передача личных данных сотрудника организации может осуществляться лишь с письменного согласия работника, а также в случаях предусмотренных законом. Потребителю информации допустим минимальный объем, по объективным причинам для выполнения определенных задач. [1]

Третьей стороне не сообщаются данные, содержащие информацию о состоянии здоровья сотрудника без письменного согласия, исключительным случаем служит угроза жизни субъекта персональных данных, иные случаи предусмотренные законодательством.

Меры безопасности при получении, обработке и хранении личной информации фиксируются как на бумажном, так и на электронном носителе. Передача данной информации недопустима по факсу и телефону.

Право доступа к личным данным работника внутри организации (внутренний) имеют: генеральный директор, руководители структурных подразделений (данные о сотрудниках своего подразделения), руководитель другого подразделения (лишь в случае перевода с одного подразделения в другое), сотрудники организации в случае выполнения служебных обязанностей, сам работник организации. Лица, имеющие доступ к персональным данным сотрудников организации определяются приказом генерального директора.

К внешнему доступу относятся потребители информации государственных и негосударственных функциональных структур, к ним относятся: правоохранительные органы и военкоматы, органы социального страхования и страховые агентства, налоговые инспекции, пенсионные фонды, подразделения муниципальных органов управления, а также органы статистики. [2]

В случае перечисления работником денежных средств, доступ к личным данным субъекта можно получить лишь с его письменного согласия.

При переходе работником на иное место работы, информация о сотруднике в другую организацию представляется при получении официального письменного запроса на фирменном бланке организации, к которому прилагается нотариально заверенная копия заявления работника.

Угроза утраты персональных данных сотрудника возникает как внутренняя, так и внешняя. Риски представляют собой как утечка информации от заинтересованного лица, так и стихийные бедствия, аварии технических средств, линий связи и другие объективные обстоятельства.

Работодатель обязан предоставить полную защиту информации персональных данных работника от неправомерного использования другими лицами, в соответствии с установленным федеральным законом.

Правила обеспечения внутренней защиты личных данных сотрудника:

- Ограниченный круг лиц, обязанности которых предусматривают работу с конфиденциальной информацией, а также распределение полномочий в работе с данными документами. Право доступа к базам данных и вычислительной технике.
- Контроль за использованием персональных данных, знание ответственным лицом нормативно-методической базы, которая предусматривает сохранение тайны и защиту информации. Наличие необходимых баз данных для полноценной работы с конфиденциальной информацией.
- Выявление нарушений системы доступа, а также порядок уничтожения секретной информации.
- Личные дела сотрудников выдаются на рабочее место генеральному директору, работника отдела кадров, специалистам структурных подразделений по письменному разрешению генерального директора.
- Документы, содержащие конфиденциальную информацию должны иметь пароль, который предоставляется руководителю службы информационных технологий.

Сотрудники организации должны быть ознакомлены с порядком обработки персональных данных, а также правах и обязанностях в данной области. Работник должен передавать достоверную информацию работодателю, состав которой установлен Трудовым кодексом РФ, а также сообщать новую информацию в случае изменений персональных данных (фамилия, присвоение нового разряда). [2]

Руководитель организации, несет ответственность за разрешение доступа к персональной информации своим сотрудникам. В тоже время, сотрудник несет личную ответственность за сохранность носителя и безопасность доверенной ему информации.

Лица, допустившие нарушение в использовании конфиденциальных сведений, несут административную, дисциплинарную в соответствии с Трудовым кодексом РФ (по усмотрению работодателя), гражданско-правовую или уголовную ответственность в соответствии с федеральными законами. [5]

Должностные лица, которые занимаются ведением персональных данных работника, обязаны обеспечивать ознакомление с материалами и документами, которые затрагивают права и свободы работника, если иное не предусмотрено законодательством. Предоставление заведомо ложной или неполной информации – влечет наложение административного штрафа на должностное лицо, в размере указанном Кодексом об административных правонарушениях. [3]

Исходя из Гражданского Кодекса, лицо, которое получило информацию незаконным способом, обязано возместить убытки (данная обязанность возлагается и на работников).

В случае нарушения неприкосновенности частной жизни, а также неправомерный отказ в предоставлении информации – влечет уголовную ответственность, либо происходит лишение права занимать соответствующие должности или деятельность. [6]

Список использованной литературы.

1. Завьялова О.В. Персональные данные сотрудника как конфиденциальная информация [Электронный ресурс] // 2013. URL: http://www.onegingroup.ru/ (дата обращения: 15.10.14 г.).

2. Защита персональных данных работника [Электронный ресурс] // 2014. URL: http://base.garant.ru/12125268/14/ (дата обращения: 14.10.14 г.).

3. Кодекс Российской Федерации об административных правонарушениях (по состоянию на 15 октября 2005 года). – офиц. текст. – Москва: Юрайт, 2005. – 333 с.

4. Персональные данные [Электронный ресурс] // 2014. URL: http://www.ispdn.ru/basis/ (дата обращения: 15.10.14 г.).

5. Трудовой кодекс Российской Федерации. – Официальное изд.. – Москва: Омега-Л, 2006. – 272 с..

6. Уголовный кодекс Российской Федерации. – Официальное изд.. – Москва: Омега-Л, 2006. – 176 с.

ПОЛОЖЕНИЕ РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ НА МИРОВОМ УРОВНЕ

А.В. Чижик

Томский политехнический университет, г. Томск
E-mail: snopic.alena@gmail.com
Научный руководитель: Барышева Г.А., доктор экон. наук

Рассмотрены показатели, влияющие на такие технологические отрасли российской промышленности как металлургическая, нефтегазовая, машиностроительная, топливно-энергетическая, химическая, и статистика страны за последние 2 года. На основе этих данных был проведен анализ и выявлен ряд факторов, мешающий развитию отраслей российской промышленности, а так же факторов, благотворно влияющих на ее развитие. Взяв за основу анализ были поставлены задачи, от решения которых зависит изменение ситуации страны в лучшую сторону.

Целью данной статьи является выявление проблематики развития отраслей российской промышленности на глобальном рынке. Особенно в таких областях как рынок инжиниринга в России, потенциал инжиниринговых компаний, подготовка специалистов для эффективного инновационного производства и обеспечения роста российской промышленности. Основными задачами я ставлю: рассмотрение отраслевой структуру хозяйства России, проведение ее оценки, выявление на основе анализа основных проблем и разработка комплекса мер в целях совершенствования государственной политики. Инжиниринг можно определить как комплекс интеллектуальных видов деятельности, в конечном итоге имеющий цель, а именно получить наилучшие (оптимальные) результаты от капиталовложений или прочих затрат, которые связанны с исполнением проектов различного направления в качестве более целесообразного подбора и эффективного применения материальных, финансовых, трудовых и технологических ресурсов в их взаимосвязи, а также способов управления и организации, на основании ведущих научно-технических достижений и с учетом конкретных обстоятельств и проектов. Инжиниринговая деятельность включает предоставление комплекса услуг производственного, коммерческого и научно-технического характера.